REMARKS

The Office Action dated 1-31 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-15, 20, 21, 27 are amended. Claims 1, 7, 12, 21, and 27 are amended to particularly point out and distinctly claim the subject matter of the invention. Support for these amendments is found at least on page 12 lines 25-26 and page 14 lines 26-30 of the specification. Claims 2-6, 8-11, 13-15 are amended to correct informalities. New claims 29-31 are added. Support for the new claims is found at least on page 13 lines 25-30, and page 20 of the specification. Thus, no new matter is added. Claims 1-31 are respectfully submitted for consideration.

The Office Action rejected claims 1, 3, 4, 6-14, 16-22, 24 and 26-28 under 35 U.S.C. 102(b) as being anticipated by US Patent No. 6,591,102 to Chavez et al. (Chavez). Applicants respectfully submit that Chavez fails to disclose or suggest all of the features recited in any of the pending claims.

Claim 1, from which claims 2-6 and 20 depend, is directed to a method for providing access to a service for a user in a communication system. A specific record, associated with the user is used at a node in the communication system, containing information which determines that a user characteristic is to be verified with a home network prior to providing access to the service.

Claim 7, from which claims 8-19 depend, is directed to a method for providing a user of user equipment with access to a service from a service provider node in a wireless communication system. A user specific record is used indicating a condition which, if satisfied, determines that a user characteristic is to be verified prior with a home network to providing access to the service. Access is provided to said service responsive to the user specific record.

Claim 21, from which claims 22-26 depend, is directed to a server node of a communication system. The server node includes means for receiving a message from a user equipment. The server node further includes means for using a user specific record, associated with the user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing said user with access to the a service. The server node includes means for generating, in response to said user specific record, an access message for providing said user with access to said service. Thus, a user of user equipment is provided with access to a service from a service provider node.

Claim 27, from which claim 28 depends, is directed to a mobile user equipment. The mobile user equipment includes means for using a user specific record associated with a user, indicating a condition which, if satisfied, determines that a user characteristic is to be verified with a home network prior to providing the user with access to a service. The mobile user equipment further includes means for generating, in response to said

user specific record, an access message for providing said user with access to said service. Thus, a user is provided with access to the service from a service provider node.

The present invention relates to a method of reducing the amount of data that must be transmitted in a communication system, while ensuring that security of the system is not compromised. To preserve the security of the system, it is necessary for the authentication/authorization of a mobile station connected to the network to be verified. This verification should be performed against data held in the mobile station's home network, as only the data held in the device's home network is guaranteed to be up to date. Some communication systems require every service request to be authorized/authenticated with the home network and this places a significant signaling traffic burden on the network and is represents an inefficient use of network resources. Other communication systems transfer the authentication/authorization data to the serving node and are then able to provide access without contacting the home network, this is the approach taken by Chavez (further discussed below). However, this approach is insecure. Any changes made to the data held in the home network, for example barring a stolen phone, will not be reflected in the copy of the data held at the serving node. The serving node will therefore continue to provide access for a barred mobile device that was previously registered with that node. In order to maintain security, it is therefore necessary to occasionally refer to the data held by the home network to verify the authorization/authentication of the mobile device. Applicants respectfully submit that the present pending claims recite features that are neither disclosed nor suggested in Chavez.

Chavez teaches a method for transmitting feature and authentication information for wireless communication services that reduces the amount of data that must be transmitted in the system. When a mobile station authenticates with a base station with a location registration request, the base station retrieves data required to authenticate the mobile station from the network and stores it in local memory for future reference. Similarly, service authorization information for a certain service is only requested by the base station when the mobile station attempts to access that service. Once received, the service authorization information is stored in local memory for future reference. The stored data can then be used to authenticate/authorize future access requests by the mobile station without needing any further information to be retrieved from the network, thereby reducing the amount of data that must be transmitted in the system.

Applicants respectfully submit that Chavez fails to disclose or suggest at least the feature of using a specific record, associated with said user, at a node in the communication system, containing information which determines that a user characteristic is to be verified with a home network prior to providing access to said service, as recited in claim 1 and similarly recited in claims 7, 21, and 27.

Instead, Chavez merely discloses authentication and authorization information is only retrieved from the network when a local copy is not available in the memory of the base station, or in other words, the user characteristic is only retrieved from the network when it is not already present in the memory of the base station. The lack of a record in the memory of the base station is not readable on "information" as recited in claims 1, 7,

21 and 27. Instead, the triggering factor in Chavez is an absence of information. Furthermore, Chavez fails to mention, disclose or suggest, "verifying" the user characteristic, as verifying implies checking that a property of a user characteristic is correct. In the system described in Chavez, data is retrieved from the network in order to determine the unknown status of a user property, not to verify its status. Thus, Chavez fails to disclose or suggest all of the features recited in claims 1, 7, 21, and 27.

Applicants respectfully submit that because claims 3, 4, 6, 8-14, 16-20, 22, 24, 26 and 28 depend from claims 1, 7, 21, and 27, these claims are allowable at least for the same reasons as claims 1, 7, 21 and 27 as well as for the additional features recited in these dependent claims.

Based at least on the above, Applicants respectfully submit that Chavez fails to disclose or suggest all of the features recited in claims 1, 3, 4, 6-14, 16-22, 24 and 26-28. Accordingly, withdrawal of the rejection of claims 1, 3, 4, 6-14, 16-22, 24 and 26-28 under 35 U.S.C. 102(b) is respectfully requested.

The Office Action rejected claims 2, 5, 15, 23 and 25 under 35 U.S.C. 103(a) as being obvious over Chavez, in view of US Patent No. 6,728,536 to Basilier et al. (Basilier). The Office Action took the position that Chavez disclosed all of the features of these claims except for the feature of transferring said information from the AAA-H to the serving node in the signaling path for the service setup and/or service event and/or registration. The Office Action asserted that Basilier disclosed this feature. Applicants respectfully submit that the cited references, taken individually or in combination, fail to

disclose suggest all of the features recited in any of the pending claims. Specifically, Chavez is deficient at least for the reasons discussed above, and Basilier fails to cure these deficiencies.

Chavez is discussed above. Basilier is directed to transmitting specific information, such as access specific roaming information and/or application specific information, between a home network and a visiting access network. The home network and visiting network are capable of communicating access independent information in a protocol, such as a AAA protocol. The access and/or application specific information is formatted in the AAA protocol. The access and/or application specific information is then transmitted over a public IP network between the home network and the visiting network. A system is provided for transmitting access and/or application information between a visiting network and a home network over a public IP network. A control access server in the visiting access network formats the access information using a secure AAA protocol to form formatted access information. An application server formats application specific information. A AAA-F server associated with the visiting network transmits the formatted access and/or application information over the public IP network to the home network. However, Basilier fails to disclose or suggest the feature of using a specific record, associated with said user, at a node in the communication system, containing information which determines that a user characteristic is to be verified with a home network prior to providing access to said service. Thus, Basilier fails to cure the deficiencies of Chavez.

Based at least on the above, Applicants respectfully submit that the cited references taken individually or in combination, fail to disclose or suggest all of the features recited in claims 2, 5, 15, 23 and 25. Accordingly, withdrawal of the rejection of claims 2, 5, 15, 23 and 25 under 35 U.S.C. 103(a) is respectfully requested.

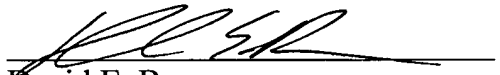
New claims 29-31 are added. Applicants respectfully submit that the cited references fail to disclose or suggest all of the features recited in claims 29-31.

Applicants respectfully submit that each of claims 1-31 recite features that are neither disclosed nor suggested in any of the cited references. Accordingly, it is respectfully requested that each of claims 1-31 be allowed and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:scw:jkm

Enclosure: Additional Claim Fee Transmittal
Check No. 14656